The Odisha Gazette

EXTRAORDINARY
PUBLISHED BY AUTHORITY

No. 1152, CUTTACK, TUESDAY, JULY 5, 2016/ ASADHA 14, 1938

ELECTRONICS & INFORMATION TECHNOLOGY DEPARTMENT

NOTIFICATION

The 1st June, 2016

Sub: Crisis Management Plan for Cyber Security in Odisha 2016.

No.1770–E&IT-V-Dev.-II-36/2016/E&IT.—

1. Introduction:

The IT sector has become one of the most significant growth catalysts for the State economy. The Government has been a key driver for increased adoption of IT-based products and solutions in the State. The crisis Management Plan is an evolving task, which needs to be regularly updated/refined in line with technological trends and security challenges posed by such technology directions. This plan caters for the whole spectrum of ICT users and providers including small and home users, medium and large enterprises and Government & non-Government entities.

1.1 Cyber-attacks & Cyber-terrorism:

Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations.

1.2 Crisis Management Plan:

Crisis Management is a critical organizational function. Failure can result in serious harm to stakeholders, losses for an organization, or end its very existence. Public relation practitioners are an integral part of crisis management teams. So a set of best practices and lessons gleaned from our knowledge of crisis management would be a very useful resource for those in public relations. Volumes have been written about crisis management by both practitioners and researchers from many different disciplines making it a challenge to synthesize what we know about crisis management and placing that in the knowledge base.

The Crisis Management Plan is prepared in line with National Cyber Security Policy, 2013. The consultation was made with the Draft Cyber Security Policy of Odisha submitted by M/s PWC (Price Waterhouse Coopers) in 2011. As there is an extant National policy on Cyber Security, it is felt that there is no requirement of a separate Cyber Security policy for the State of Odisha. Therefore, the attempt is made to prepare Crisis management plan for cyber security and create institutional mechanism to address the cyber security issues.

1.3 Purpose and scope:

The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical business functions and processes of the Government of Odisha. Apart from this, the other purposes are:—

a) To ensure that interruption or manipulations of critical functions/services in critical sector organizations of the State are brief, infrequent and manageable and cause least possible damage.

b) To enable respective administrative Departments to draw-up their own contingency plans in line with Crisis Management Plan for countering cyber-attacks and cyber terrorism, equip themselves suitably to implement, supervise implementation and ensure compliance among all the organizational units within their domains.

c) To assist organizations to put in place mechanisms to effectively deal with cyber security crisis and be able to pin point responsibilities and accountabilities right down to individual level.

This plan takes into consideration the crisis that occurs due to cyber security incidents and breaches, and presents a broad based approach to deal with such crisis. The approach and methodology of this Crisis Management Plan are derived from the “Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism” prepared by Department of Electronics and Information Technology (DeitY), Government of India.

The field of cyber security is technology intensive and new vulnerabilities emerge with progress in technology giving rise to new types of incidents. As such, the plan of response to cyber security incidents needs to be updated on regular basis, preferably once in a year.

The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism describes the following aspects:

a) The Critical Sectors, Nature of cyber crisis and possible targets and impact of particular type of crisis on these targets.

b) Crisis due to focused cyber-attacks affecting the organisations in critical sector such as Defence, Energy, Finance, Space, Telecommunications, Transport, Public Essential Services and Utilities, Law Enforcement and Security.

c) Different Types of cyber crisis described include Large-scale defacement and semantic attacks on websites, Malicious code attacks, Large scale SPAM attacks, Spoofing, Phishing attacks, Social Engineering, Denial of Service (DoS) and Distributed DoS attacks, attacks on DNS, Applications, Infrastructure and Routers, Compound attacks and -High Energy RF attacks.

d) Measures to be taken at organisational level for enhancement of security posture of Information and Network including implementation of Information Security Best Practices based on ISO 27001 standard, provisioning for Business Continuity Plan and/with Disaster Recovery, Awareness building and Security Training.

e) Incident handling and Management, Sharing of information pertaining to incidents and conducting mock drills to test the preparedness of Critical Infrastructure organisations to withstand cyber-attacks.

2. Cyber Crisis and Contingencies:

This section identifies different types of threats and crises that affect specific targets. Impact of such crisis on respective targets and critical business functions and services of Government of Odisha are identified to determine suitable response and mitigation actions.

While preparing the CMP the following actions are kept in mind:

a. Identification of all organizational units under the domain of Government of Odisha
b. Functions and services of the organizational units
c. Inventory of all Critical Information assets
d. Risk Assessment and risk management (Ref. ISO 27005:2008)
e. Business Impact Analysis (Ref. BIA template at ***Appendix E***)
f. Contingency plan for IT systems (Ref. Contingency plan template at ***Appendix F***)

Cyber crisis has unique features that are different from a physical crisis. In some cases, the severity of cyber crisis is high but confined to individuals or few organisations in a limited area. In other cases the severity may be low but widely spread to a larger area.

2.1 Types of Cyber Crisis:

There are various types of cyber security incidents that can trigger a crisis at individual/organization, multiple organizations or State level.

a) **Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure:** Publicly available reconnaissance techniques, including web and newsgroup searches, WHOIS querying, and Domain Name System (DNS) probing, are used to collect data about the structure of the target network from the Internet without actually scanning the network or necessarily probing it directly.

b) **Large scale defacement and semantic attacks on websites:** A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website. Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated.

c) **Malicious Code attacks (virus/worm/ /Trojans/Botnets):** Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, trojans, spyware, adware and Bots.

d) **Malware affecting Mobile devices:** Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile, Blackberry OS.

e) **Large scale SPAM attacks:** Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems.

f) **Large scale spoofing:** Spoofing is an attack aimed at 'Identity theft'. Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

g) **Phishing attacks:** Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

h) **Social Engineering:** Art of manipulating people into performing disclosure actions or divulging confidential information.

i) **Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks:** DoS is an attempt to make a computer resource unavailable to its intended users. A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system.

j) **Application Level Attacks:** Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases.

k) **Infrastructure attacks:** Attacks such as DoS, DDoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralised/Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware.

l) **Compound attacks:** By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber-attack.

m) **Router level attacks**: Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication.

n) **Attacks on Trusted infrastructure:** Trust infrastructure components such as Digital Certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks.

o) **High Energy Radio Frequency Attacks:** Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service.

p) **Cyber Espionage and Advanced Persistent Threats:** Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware.

For details on nature of cyber crisis, possible targets & impacts refer ***Appendix-K***

2.2 Critical Sector / Organizations in State Government:

Many departments of the State Government have implemented e-Governance projects which are critical to function of the department and delivery of services to citizens. The organizations are identified to accord appropriate priority in developing medium to combat cyber-attacks.

The following key sectors/key organizations have been identified:

- Law enforcement agency
- Citizen Data (UID)
- IT Department
- Finance Department
- Revenue Department
- Commerce and Transport
- Odisha State Data Centre
- Odisha State Wide Area Network
- Secretariat LAN
- Banking organization
- Communication & ISP organization

These sectors/organizations would include Government organizations including State PSUs. This list may be revised from time to time.

3. Organizations for Crisis Management:

CERT-In (the Indian Computer Emergency Response Team) is a Central Government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the Country. This plan proposes State level organization structure to add all State level crisis. They are SCMC (State Level Crisis Management Committee) the apex body to cater to the major crisis of higher importance and CERT-O (Computer Emergency Response Team –Odisha) for sectorial CERT for monitoring & resolving various issues on cyber-attack in the State in line with the CERT – In.

3.1 Indian Computer Emergency Response Team (CERT-In):

CERT-In monitors Indian cyberspace and coordinates, alerts and issues warning of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the Country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs all over the world; and Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the Country.

3.2 State Level Crisis Management Committee (SCMC):

Government has already formed a committee vide notification to 2488 dt. 15/09/2014 of Home Department to oversee the implementation of Crisis Management Plan. This committee shall also act as State Level Crisis Management Committee (SCMC). This committee is an apex body of high-level officials of the Odisha Government for dealing with a crisis, which has serious or national ramifications, will also deal with State level crisis arising out of focused cyber-attacks. This committee shall monitor, review the Cyber Security Plan of the state, and oversee the Crisis Management plan on Cyber Security, critical information Infrastructures, etc. and other cyber related subjects. The composition of the Committee is as under:

A.	Secretary, Home Dept.	Chairman
B.	Secretary, E&IT Dept.	Member
C.	Chief Information Security Officer(CISO)	Member
D.	Representative from CERT-In Govt. of India, New Delhi	Member
E.	Director, IIIT or his/her Representative	Member
F.	SIO or his/her Representative, NIC, Bhubaneswar	Member
G.	Special Secretary, E&IT Dept.	Member Convener

The SCMC will be free to co-opt members depending on the nature of crisis, as and when required. When a situation is handled by the SCMC it will give such directions to *the* Crisis Management Group of the Department as deemed necessary. This committee shall also act as Information Security Steering Committee (ISSC) as proposed by NCIIPC.

3.3 Cyber Security through CERT-O:

As per the Crisis Management Plan for countering cyber-attacks and cyber terrorism prepared by Government of India, State draw up their own sectoral Crisis Management Plans and implements the same. Since there is lack of adequate expertise in Government/Government

Agencies/ it emerged that there is need for setting up an ongoing permanent mechanism which would act as nodal agency for monitoring various cyber security related matters for Government of Odisha/ Government Organisations. The State Government has therefore felt the necessity for setting up of Computer Emergency Response Team-Odisha (CERT-Odisha or CERT-O) in line with CERT India (CERT-IN) to cater to crisis situations in Cyber Security matters of Government of Odisha.

3.3.1 Creation of CERT-O : CERT-O should be a unit of E&IT Department, Government of Odisha with following members as its Governing Body:

(a) Principal Secretary, IT Deptt.	… Chairman
(b) Representative from CERT-In,GoI	… Member
(c) One expert from IIT,Bhubaneswar / IIIT,Bhubaneswar….	Member
(d) CiSO or representative of CISO	... Member
(e) Head CERT-O	….. Member Convener
(f) Two experts on Cyber Security	…Member

For eligibility criteria for security experts refer ***Appendix N:***

The modalities to establish CERT-O may be finalized by E&IT Department, Govt. of Odisha. OCAC being the nodal agency & Technical Directorate of I.T. Department, Govt. of Odisha will facilitate the provisions for IT infrastructure & support to the CERT-O. At present the CEO, OCAC or any person nominated by the Govt. may head the CERT-O initially to start with.

3.3.2 Objectives of CERT – O:

i. To formulate State's crisis management plan as appropriate from time to time and implement the same in coordination with CERT-In & with direction of SCMC.

ii. To initiate proactive measures to increase awareness and understanding of Information security and computer security issues throughout the community of network users and service providers by disseminating security related information.

iii. To act as a nodal agency to conduct security audits or assessments of Government and constituent IT infrastructure in the State, evolving security policy for the State.

iv. To act as a central point for monitoring, identifying vulnerabilities and suggesting remedial measures for correcting vulnerabilities in computer and communication systems(websites & e-governance applications) belonging to government and 'certify' any e-governance or e-commerce site in the State

v. To conduct education, training, research and development.

vi. To collect and maintain a repository of all System/Website administrators of Odisha Government Websites/Web applications.

vii. To build capacity among the technical personnel to identify and fight security threats.

viii. To assist SCMC by priority with relevant information for their decision making process.

ix. To carry out direction of SCMC to fight cyber attacks.

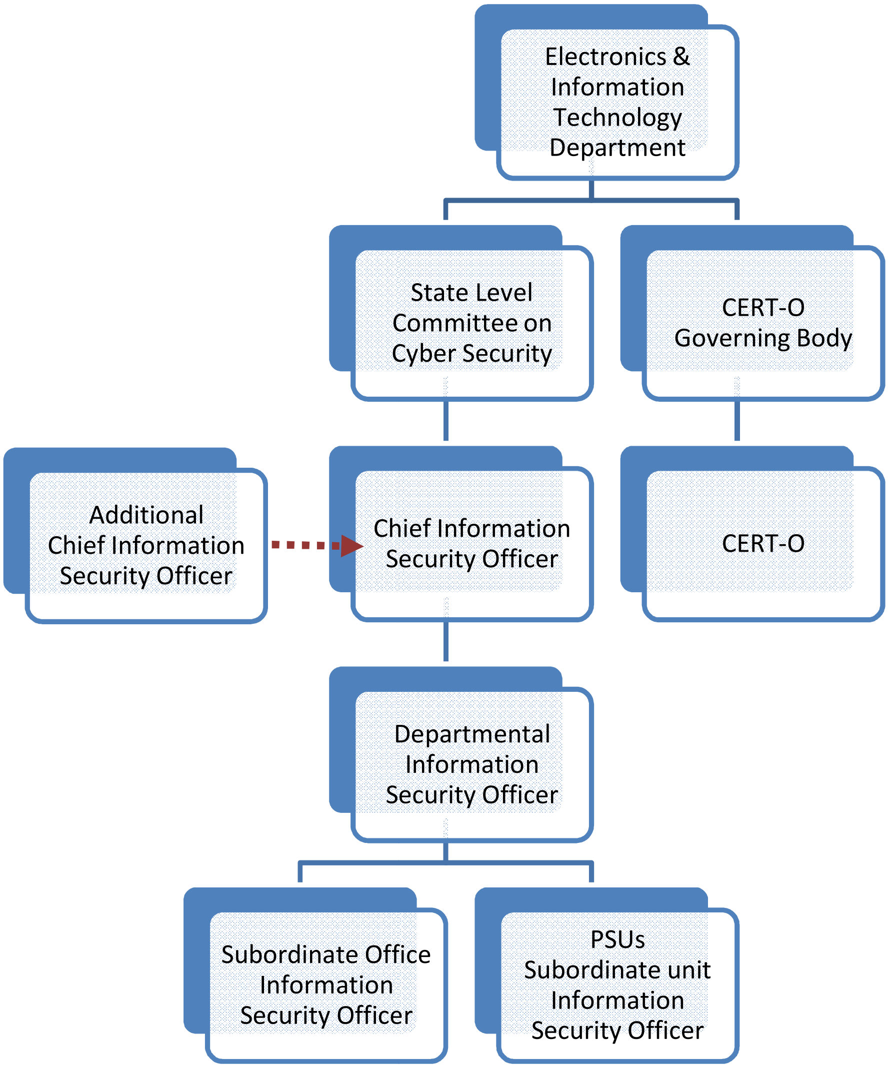
x. To create a suitably qualified and empowered personnel who can further enhance knowledge and expertise in this area to advance the mission.

3.3.3 Roles & Responsibilities of CERT-O:

- Vulnerability Reporting
- Incident Reporting
- Penetration testing
- Incident Analysis
- Vulnerability Assessment of various Odisha Government Websites
- Log analysis
- Coordination with CERT-In, OCAC, other State Government departments and SCMC
- Identify and classify cyber-attack scenarios.
- Determine the tools and technology used to detect and prevent attacks.
- Develop a checklist for handling initial investigations of cyber-attacks.
- Determine the scope of an internal investigation once an attack has occurred.
- Conduct any investigations within the determined scope.
- Promote cyber security awareness within departments.
- Address data breach issues, including notification requirements.
- Conduct follow up reviews on the effectiveness of the department's response to an actual attack.
- Prepare SOP for different types of crisis.
- Head CERT-O shall formulate appropriate guidelines and action plan to ensure the role and responsibility of CERT-O as described above.

3.4 Institutional Framework:

It is essential to implement the CMP from the grass root level for countering Cyber threats. In view of this it is proposed to have Information Security Officers (ISO) at the subordinate office, PSUs and Departments. These ISOs shall report to Chief Information Security Officer (CISO) of the State who will be assisted by Addl. CISO. The day-to-day Security related activities for the State will be looked after by CERT-O. CERT-O will be a unit under the administrative control of E&IT Department and will have a Governing Body for its management. The ISOs will continuously interact with CERT-O for Cyber security related assistance. CERT-O and CISO shall closely work to mitigate the Cyber Security issues. State Level Committee on Cyber Security shall be the apex committee for Crisis Management in the State. The same committee shall also act as Information Security Steering Committee (ISSC) as per mandate of National Information Security Policy and Guidelines.


Electronics & Information Technology Department
State Level Committee on Cyber Security
CERT-O Governing Body
Additional Chief Information Security Officer
Chief Information Security Officer
CERT-O
Departmental Information Security Officer
Subordinate Office Information Security Officer
PSUs Subordinate unit Information Security Officer

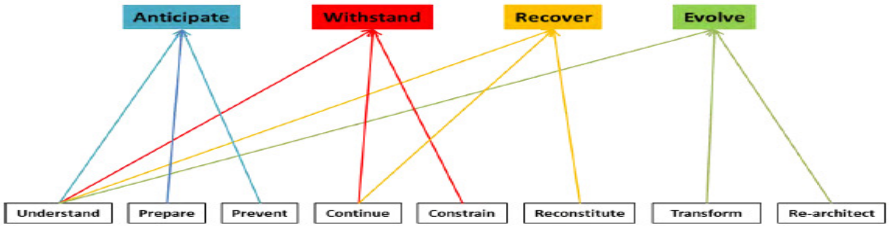
4 Prevention Strategies & Plans:

4.1 Cyber resilience of Individual Organisations:

Cyber resilience is defined as ability of organization or business process to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact of such cyber-attacks.

4.2 Principles of resilience:

At a conceptual level, the goals and principles can be shown as in the following diagram:



Cyber resiliency goals and principles

4.3 Protection and resilience of Organization's infrastructure:

To build cyber resiliency, State Government organization need to work for the following:

- Identification of key information and technology assets that support the services of that organization.
- Implementation of controls to protect those assets from cyber attack
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption.
- Development of processes to maintain and repeatedly carry out the protection and recovery activities.
- Development of appropriate measures to drive these activities
- To develop a plan for protection of organization Infrastructure and its integration with business plan and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To closely interact with 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) by providing it the necessary and timely information.
- To ensure identification, prioritization, assessment, remediation, and protection of organization infrastructure and key resources based on the plan for organization Information Infrastructure.
- To ensure compliance to global security best practices, business continuity management and cyber crisis management plan by all entities within domain of organization/ department, to reduce the risk of disruption and improve the security posture.

4.4 Cyber Resilience components & control matrix:

A matrix, showing relation between each of the components within system and their mapping to these controls, may be referred at **"*Appendix I*'.**

4.5 Mock Drills to test preparedness to withstand cyber attacks:

The State Government organisations should conduct as well as participate in simulated cyber event exercises on their networks and system infrastructure to test their preparedness in respect of response, coordination and recovery mechanism to the simulated cyber security breaches, with the help of CERT-In / CERT-O and OCAC.

Periodic Mock Drills – Depending on the Criticality of Department Application/Infrastructure.

4.6 Incident Prevention and Precautionary Measures:

The organizations/Units within the domain of Government of Odisha should implement the following as precautionary measures to prevent cyber security incidents, Refer "***Appendix L".***

4.7 Deployment of Information Security experts:

Given the size of the problem and increasing threats of cyber terrorism, there is a need to deploy more experts in this field. A large number of security experts could be working on emerging vulnerabilities and effective defences. Periodic training may be provided to information security experts to update the skills with respect to latest technologies/threats and implementations.

4.8 IT Security Best Practices Compliance-Levels of Assurance:

In order to assist organizations in government as well as critical sectors to follow a roadmap for progressively achieving compliance and assurance w.r.t. IT security best practices, different levels of assurance have been conceived. Using these levels of assurance and the methods of verification, organizations can carry out self-assessment with regard to their present status of compliance assurance and declare the same accordingly. It is expected that these levels of assurance will also help the organizations in improving the maturity of their IT security management system as well as enhancing predictability and proactive nature of their system. Levels of Assurance are available at "***Appendix J***'.

NB: Government of Odisha *is at level 2 as on Year 2014. (Refer Appendix J)*

5 Crisis Recognition & Mitigation Plan:

5.1 Classification – Levels of Concern:

The crisis arising out of cyber-attacks are categorised and prioritised from **level 1 to Level 4**. The levels of Level of concern are mentioned below:

i. **Level 1 -** *Guarded*
Scope: Individual Organisation

ii. **Level 2 -** *Elevated*
Scope: Multiple Organisations

iii. **Level 3 -** *Heightened*
Scope: State/Multiple States

iv. **Level 4 -** *Serious*
Scope: Entire Nation

*Refer **Appendix M** for details on Levels of Concern*

5.2 Reports Mechanism:

As and when a cyber-crisis situation develops, respective organizations will immediately convey to the State Government through any quickest possible means. Further, all organizations will take all necessary actions as given in **Appendix B** of this document and also report the incident to CERT-In in the manner and format as prescribed in **Appendix G** of this document.

5.3 Control Room of the State:

Government of Odisha will setup a Control Room which would be activated immediately after a crisis situation is reported. A senior officer from the existing hierarchy of State Govt. should be designated as in-charge of Control Room who would draw up a plan for its manning during crisis situations on a 24 X 7 hour basis. Hot line facilities wherever necessary may be setup in consultation with the Department of Telecommunications. There would be a well laid out drill for the Control Room and the personnel expected to man it should be adequately trained in Control Room duties. Names, telephone numbers, cellular mobile phone numbers and addresses of Members and Alternate Members of State Government and various stake holders will be kept in the Control Room**.**

5.4 Response System:

Immediately on the occurrence of a crisis, the Contingency Plan would be put into effect by the respective organizations. The response action will be initiated in consultation with CERT-O / CERT-In, if the situation has wider ramifications and warrants response at the State/National level. The State Govt. would activate its Control Room and summon a meeting of the Crisis Management Group to oversee the implementation of its Contingency Plan.

A sample SOP (Standard Operating Procedure) to handle Website defacement is explained in ***Annexure C*** *of the document. Further SOPs will be prepared for different types of crisis by CERT-O in due course of time to deal with them efficiently.*

5.5 Mitigation Strategy:

General Guidelines on Crisis Management and security of Critical Infrastructure are outlined in ***Appendix H***. The table outlines the nature of crisis/contingency affecting the systems of individual organisation, multiple organisations, States and Nation leading to crisis of different levels and authorities responsible for mitigation along with agencies that support mitigation actions. The steps necessary to mitigate crisis will vary with respect to nature and severity of crisis. Respective authorities responsible for mitigation of a crisis will report the incident to the designated supporting organisations and step-wise approach for mitigation *vis-à-vis* nature of crisis/contingency as given in the table in ***Appendix H*.**

5.6 Media Management:

A media forms a vital link between those responding to crisis situation and the outside world. Besides this, media also can help in educating all concerns about crisis prevention and preparedness. It is recognized that unbased and comprehensive media coverage can effectively aid the crisis response & resolution process and also enhance public confidence in the ability of organisations to respond to crisis. Accordingly media management is a crucial issue in terms of pre-incidents as well as post incident information flow. In order to make best possible use of this vital link, it is necessary that media is given clear information and regular updates to enable them to perceive right picture and proportion of the crisis. In this context, the organisations responding to cyber security incidents shall identify responsible person of suitable level who has access to correct and updated information and is adequately trained for proper and consistent communication and avoid contradiction at all times.

5.7 Closing the incident and Information Sharing:

After successful mitigation and recovery from incident, the following need to be undertaken (before closing the incident) for future reference/precaution:

- Perform a post-mortem analysis of the incident as well as the incident response adopted at the organisation , CERT – O and CERT-In level.
- Evaluate and perform assessment of the attack from the technical point of view in order to fine-tune and optimize the eradication mechanism.
- Document lessons learnt from the incident and prepare incident report, including infrastructure protection improvements from the post-mortem process.
- Share incident report with CERT-In for future precaution and mitigation of similar attacks
- All critical organisations/departments shall implement infrastructure protection improvements resulting from post-mortem reviews or other protection improvement mechanisms.

5.8 Contact Information:

Names, telephone numbers, cellular mobile phone numbers, e-mail IDs and addresses of Members and Alternate Members of various stakeholders are given in the ***Annexure B*** respectively.

6. Conclusion:

Under circumstances it remains to be seen what shape counterattacks will take, but under the mounting pressure to do something about it, their continued emergence is inevitable, as statistics pour out about how much cybercrime costs the State. Hackers have been able to have free run of the internet, only being brought in if they make a silly mistake. Adequate Counter measures will not only help deter attacks when they happen, but more importantly, deter hackers from launching them in the first place. It will take years for legal systems to set preference and formalize their thoughts on these matters, and equally long or longer for inter-jurisdiction litigation to proceed effectively. For all these reason the Crisis Management Plan for Countering Cyber-attacks and cyber terrorism for the State need to be in place.

Appendix-A

A. Incident Handling Team Structure:

A.1 Notification Team :

An incident can be reported by anyone; however it is typically reported by one of the following persons/ groups in the organisation/department involved in managing and monitoring resources/ services:

- IT Infrastructure [particularly Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) / Router Monitoring Team]
- Network & System Support (NSS) Engineers
- Web/System/Network Administrator
- Administration (Physical Security) Team
- Internal / External Audit Team
- Associates

Responsibility:

An Associate / team discovering the incident is responsible for communicating the same to the Service Desk Team immediately. Incidents must be assigned the appropriate severity level by the associate / team at the time of reporting the incident.

A.2 The Service Desk Team:

The Service Desk is the place in the organization where all security incidents are to be registered by issuing a service ticket. Efficient and effective reaction to security incidents demands a formal method of working that can be supported by software tools.

Incidents that cannot be resolved immediately by the Service Desk are to be assigned to the concerned functional group for that location. A resolution or work-around should be established as quickly as possible in order to restore service to users with minimum disruption to their work. After resolution of the cause of the incident and restoration of service, the incident is closed.

Throughout an incident life cycle it is important that the service ticket is maintained. Even in cases where the incident is reported by a phone call / email, the ticket must be raised by the service support team member. This allows any member of the support team to provide an up-to-date progress report.

A.3 Crisis Detection and Prevention:

Crisis detection and prevention is ensured 24 hours a day via the Administration, Human Resource and Information Security staff together with all involved project delivery staff. All these services would co-operate towards the prevention and handling of a crisis. It is the concerned associate on duty who is responsible for alerting the Crisis Management Cell (CMC) of an imminent serious crisis.

A.4 Level I Incident Resolution Team:

Each organisation should have an identified list of personnel who will be part of the respective Level-I Incident Resolution team.

Responsibilities:

- Limit the access to systems and networks from outside in consultation with ISPs
- Monitor and detect anomalous behaviour and degradation of services
- Identify the correctness of the severity level
- Take all logs of affected systems for analysis
- Correct, Eradicate and Recover
- Seek necessary resources and support from the corresponding Level-II Incident Resolution Team.
- Provide regular updates to corresponding Level-II Incident Resolution Team and the Crisis Management Cell (CMC) regarding progress of the incident handling process.
- Escalate to the corresponding Level-II Incident Resolution Team, if unable to resolve within the prescribed time frame/reasonable time frame.

A.5 Level II Incident Resolution Team:

The team involves concerned department's official , Admin, HR functional groups and CERT-O. This team have full authority to undertake any actions or decisions necessary to contain, eradicate and recover the situation.

Responsibilities:

- Provide support to the Level-I Incident Resolution Team to facilitate prompt containment, eradication and recovery of the affected entity.
- Communicate to all responsible parties and stakeholders like Project Managers including System Integrator (if warranted in the agreement) and Crisis Management Cell (CMC) within the organization.
- Maintain contact with CERT-O and CERT-In and the respective nodal agency.
- Supervise and coordinate all security incident handlings for the functional group at the particular location and facilitate experience and information sharing on security incident to SCMC, CERT-In and respective nodal agency.

Appendix- B

B. Incident Response activities during the First Hour:

B.1 Introduction:

The primary objective of incident response actions during first hour is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services of the organisation.

The following guidelines describe the actions to be taken within the affected organisation during the first hour of incident. The guidelines also facilitate detailed incident analysis and determination of recovery and response actions and possible escalation within and outside the organisation.

B.2 Triggers for first reaction:

The reaction by the users or administrators within an organisation could be triggered by observation of certain symptoms and anomalies in the functioning of systems, networks and processes. The trigger for response action could be infection, attack or intrusion or malfunctioning of a system or reported loss of damage to information assets/systems etc. Further the actions could be triggered when alerts are received from external organisations such as CERT-In and other Incident Response teams and security agencies.

B.3 Means of Detection:

The means of detecting anomalies and abnormal conditions that require response actions are Users, System/Network Administrators, technical tools and external alerts from security agencies such as CERT-In/CERT-O.

B.4 Symptoms of incidents and response actions:

Table 3.1 outlines the general symptoms indicating occurrence of incident noticeable by all types of users, source of detection, response actions required and persons responsible for the actions.

Table 3.2 outlines Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection mechanisms and response actions required and authorities responsible for the actions.

Table 3.1 General symptoms of incidents noticeable by all types of users & System Administrators and related response actions:

Symptoms/Alerts	Source of detection	Response actions	Who to handle
(1)	(2)	(3)	(4)
Common Symptoms			
• Non-availability of computer system (failure to start)	• User	• Boot with alternate OS/ recovery media. • Check the booting process for specific errors. • Report to the System administrator	• User • System Administrator
• Frequent system crashes • Unexplained, poor system performance • Presence of new files • Presence of unknown processes • Changes in the file size or dates •	• User	• Scan system with updated Antivirus & Anti-spyware • Report to the System administrator	• User • System Administrator
• New suspicious user accounts •	• User	• Report to the System administrator	• System Administrator
• Failed or successful social engineering attempts	• User • System Administrator	• Collect all details such as email content, header etc and examine. • Alert other users	• System Administrator
• Failed log in attempts by unauthorized users	• Technical tools • Supervisory review of logs	• Determine the timing, sources of activities • Trace the attack sources from logs of system/directory server.	• System Administrator
• Unusual time of usage • Unauthorized user accounts	• Supervisory Review of logs	• Correlate with physical access by users • Correlate with logs of perimeter devices to find external intrusion	• System Administrator • Network Administrator
• Virus/worm infection	• User • System Administrator	• Disconnect system from network • Boot with different OS and scan with Antivirus & Anti-spyware • Antivirus and Anti-spyware should be updated regularly	• User • System Administrator

(1)	(2)	(3)	(4)
• Suspicious probes	• Technical tools (IDS/IPS/Firewall)	• Close the ports and services which are not required • Send the logs to Incident Response team for examination	• Network Administrator
• Abnormal surge in traffic (inbound/outbound)	• Technical tools • Network Behaviour Analysis • Router	• Trace the specific service/protocol • Detect the source of generation of abnormal traffic • Correlate with alerts from CERT-In/CERT-O	• Network Administrator
• External Alerts			
• Alert for new vulnerability	• CERT-In/CERT-O	• Apply appropriate patches/updates • Implement suggested workarounds for zero-day vulnerabilities	• System Administrator
• Alert on propagation of malicious code	• CERT-In/CERT-O	• Update the Antivirus signatures • Follow the countermeasures suggested in the specific advisory and in this table	• System Administrator
• Alert indicating attack sources	• CERT-In/CERT-O • Security agencies	• Block the attack sources notified by CERT-In/CERT-O and other agencies	• Network Administrator

Table 3.2 Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection mechanisms and Response actions

Symptoms/Indications/Alerts	**Source**	**Response actions**	**Who to handle**
Website defacement and semantic attacks			
Detection of defacement/intrusion of website	• Users • Website administrators • External agencies	• Disconnect the web server hosting defaced/compromised website • Examine the compromised system/website for specific unauthorized changes • Restore the website content, Shift and run website from a different trusted system by making appropriate DNS changes at the new system • Collect relevant logs of server and application and submit to IR team of organisation • Report the incident along with logs to CERT-In/CERT-O	• Website Administrator • Network Administrator

Malicious Code attacks (virus/worm/ /Trojans/Bot nets/Spyware)			
• Unexplained poor system performance • Presence of suspicious process/files on system • Surge in traffic on ports/services used by malware • Connections to suspicious remote systems • Unusual ports open	• Users • System Administrator • Alerts from Antivirus, NIDS • External agencies	• Disconnect infected systems from network • Scan with updated Antivirus and Anti-spyware • Apply appropriate countermeasures in consultation with CERT-O / CERT-In	• System Administrator
SPAM attacks			
• Abnormal surge in SMTP traffic • Bandwidth congestion • Slow response of mail servers	• Users • Network Administrators • Network Behavior Analysis	• Check the mail servers for open relays and disable • Close ports not required in the Mail server • Identify possible sources of Spam from email headers and invoke blacklists such as SBL, XBL and PBL • If attack persists report to CERT-O /CERT-In	• Network Administrator • Mail server Administrator
Attacks on Mail Servers			
• Non availability mail accounts • Compromised mail accounts	• Users • Mail server administrator	Mail server compromise: • Disconnect mail server • Activate standby mail server • Check logs of mail server and identify attack source • Send the logs to CERT-O / CERT-In User account compromise: • Reset the password • Enforce strong passwords (minimum 8 digit and alphanumeric) • Enforce email best practices	• Mail server Administrator
Identity Theft Attacks through spoofing			
• Detection of suspicious network connections • Detection of Packets with suspicious source address • Emails from masqueraded account name	• Alerts from IPS/IDS • Email headers	• Examine the email header and find the actual origin of email • Notify and alert users • To counter spoofing, implement Egress and Ingress filtering at perimeter (Router) • Enforce email authentication • Report to CERT-O/CERT-In	• Network Administrator

Phishing attacks			
• Reporting of phishing email/website	• Users • Antiphishing/ fraud detection services • CERT-In/ external agencies	• Report phishing incident to CERT-O /CERT-In • Report phishing URL to phishing filters • Send phishing emails and details of phishing website to CERT-In/ CERT-O	• Users • Designated persons
Denial of Service (DoS) attacks			
• Non availability of services such as website, email etc • System crashes • Bandwidth congestion • Surge in traffic	• Users • Website Administrator	• Identify the type of attack such as flooding of particular types of packets/requests (TCP SYN, ICMP etc.) by examining logs of Router/IPS/IDS/ Firewall • Identify the attack sources • Block the attack sources at Router/Packet filtering device • Check Router configuration and implement Egress and Ingress filtering to block spoofed packets • Disable the non-essential ports/services • Report to CERT-O /CERT-In with relevant logs	• Network Administrator • Website Administrator
Distributed Denial of Service (DDoS) attacks			
• Non availability of services such as website, email etc • System crashes • Bandwidth congestion • Surge in traffic	• Network Administrator • Alerts of IPS/IDS/ Firewalls • Network Behaviour Analysis • CERT-In	• Identify the type of attack such as flooding of particular types of packets/requests by examining logs of Router/IPS/IDS/ Firewall • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • If problem persists shift web/mail services hosting to alternate Internet Protocol addresses (IPs) • Report to CERT-O/CERT-In with relevant logs	• Network Administrator

DoS Attacks on DNS server			
• Slow response or non-availability web/mail services	• User • Network Administrator	• Change the Primary DNS Server • Implement Source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Run separate DELEGATED and RESOLVING name servers • Disable Recursion on DNS server authoritative for the zone • Restrict zone transfers to Secondary name servers only • Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. • Report to CERT-O /CERT-In	• Network Administrator
DNS Cache poisoning attacks			
• Redirection of legitimate web/mail traffic to suspicious websites/mail servers	• User • Network Administrator	• Purge cache • Restart DNS server • Replace DNS records with content from trusted backup • Examine DNS forwarding traffic to identify rogue DNS server and block • Restrict rights of configuration changes to Administrator only • At client side, delete any additional entries in HOSTS file • Report to CERT-O /CERT-In	• Network Administrator
Application Level attacks			
• Unauthorised changes to Data • Suspicious user activity • Elevation of privilege of user accounts • Presence of malicious links/ content	• Web/ Database Administrator • Application logs	• Disable suspected user accounts • Reduce the interactive features and run with minimum essential features • Restore data from trusted backup • Identify attack sources from application logs and block • Enforce Input validation • Apply latest patches/updates • Report to CERT-O /CERT-In	• Web Administrator • Database Administrator

Router level attacks			
• Unexplained packet loss • Non availability of gateway/ Internet services	• Users • Network administrator • Review of Router configurations	• Replace the router with a securely configured standby router with Egress and Ingress filtering • Check the logs and configuration files of compromised router to identify attacks • Replace the configuration files with trusted back-up • Apply appropriate patches/ updates • Block the attack source • Report to CERT-O / Service Provider/CERT-In	• Network Administrator
High Energy RF based Denial of Services Attacks			
• Non availability of wireless connectivity • Degraded Signal to Noise Ratio • Increased Noise levels in the airwaves	• Users • Network Administrator • Alerts of IDS/IPS	• Identify the other devices due to which RF interference occurs and physically remove them. • Detect rouge access points and remove them • If attack persists switch critical functions to wired networks • Report to CERT-O /CERT-In	• Network Administrator
Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure			
• Huge amount of IPS/IDS alerts • High volume of dropped packets by Firewalls • Surge in specific traffic	• User • Network Administrator • Logs of relevant devices	• Identify the type of scans/probes by examining logs of Router/IDS/ IPS/ Firewall • Identify the sources of scans • Block the sources of scanning • Report the incidents with relevant logs to CERT-In/ CERT-O	• Network Administrator

B.5 Conditions for escalation and detailed analysis:

It is quite possible to come to a conclusion that there would be situations that call for:

- Actions within the organisation
- Actions beyond an organisation

The users observing the symptoms/indications mentioned in Table 3.1 and 3.2 should immediately report the same to concerned system/network administrator or designated authority with in the organisation.

The System/Network administrators should escalate the reports of incidents affecting or could affect critical business functions or services to appropriate authorities within the organisation, CERT-O and CERT-In.

After the response actions within 1st hour of incident, the procedures and actions described in the ***Appendix V*** “Incident response during first 24 hours” of CERT-In/CERT-O need to be followed for detailed incident analysis and follow-up actions.

B.6 what needs to be reported to CERT-In/CERT- O:

The following cyber security incidents must be reported to CERT-In/ CERT- O in the format prescribed in ***Appendix G*,** within one hour of occurrence of the incident or noticing the incident.

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unathorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.

Appendix - C

Guidelines on Crisis Management and Security of Critical Infrastructure

C.1.0 Introduction:

Critical networks contain computers and applications that perform key functions in providing essential services and commodities. As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyber space today. By allowing remote collection and analysis of data and control of equipment, critical networks provide great efficiency and are widely used. However, this makes critical networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure.

C.2.0 Guidelines to improve security of critical networks:

The guidelines prescribed in the following sections are intended to ensure that interruptions or manipulations of critical functions/services in critical sector organizations are brief, infrequent, and manageable and cause least possible damage.

The following steps focus on specific actions to be taken to improve the security of critical networks:

C.2.1 Identify all connections to critical networks:

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the critical network. Develop a comprehensive understanding of all connections to the critical network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

C.2.2 Disconnect unnecessary connections to the critical network:

To ensure the highest degree of security of critical systems, isolate the critical network from other network connections to as great a degree as possible. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the critical network must be a primary goal to provide needed protection. Consider 'Air-Gap' for sensitive networks, following a risk assessment.

Strategies such as utilization of “demilitarized zones” (DMZs) and data warehousing can facilitate the secure transfer of data from the critical network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

C.2.3 Evaluate and strengthen the security of any remaining connections to the critical network:

Conduct penetration testing or vulnerability analysis of any remaining connections to the critical network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the critical network. Since the critical network is only as secure as its weakest connecting point, it is essential to deploy firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the critical network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted “blanket” network access simply because there is a need for a connection to certain components of the critical system. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organisation management must understand and accept responsibility for risks associated with any connection to the critical network.

C.2.4 Harden critical networks by removing or disabling unnecessary services:

Critical control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when critical networks are interconnected with other networks. Do not permit a service or feature on a critical network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from critical networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are available in the public domain. Additionally, work closely with critical vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

C.2.5 Do not rely on proprietary protocols to protect your system:

Some critical systems use unique, proprietary protocols for communications between field devices and servers. Often the security of critical systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little “real” security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, it may be demanded from vendors to disclose any backdoors or vendor interfaces to your critical systems, and expect them to provide systems that are capable of being secured.

C.2.6 Implement the security features provided by device and system vendors:

Older critical systems (most systems in use) have no security features whatsoever. Critical system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer critical devices are shipped with basic security features, but these are usually disabled to ensure ease of installation.

Analyse each critical device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

C.2.7 Establish strong controls over any medium that is used as a backdoor into the critical network:

Where backdoors or vendor connections do exist in critical systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the critical network and remote sites. Successful “war dialing” or “war driving” attacks could allow an attacker to bypass all other controls and have direct access to the critical network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of call back system.

C.2.8. Implement internal and external intrusion detection systems, incident response system and establish 24-hour-a-day incident monitoring:

To be able to effectively respond to cyber-attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

C.2.9 Perform technical audits of critical devices and networks, and any other connected networks, to identify security concerns:

Technical audits of critical devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the “paths of least resistance” that an attacker could exploit.

Analyse identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyse this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems.

C.2.10 Conduct physical security surveys and assess all remote sites connected to the critical network to evaluate their security:

Any location that has a connection to the critical network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the critical system. Identify and assess any source of information including remote telephone/computer network/fibre optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow “live” network access points at remote, unguarded sites simply for convenience.

C.2.11 Establish critical “Red Teams” to identify and evaluate possible attack scenarios.

Establish a “Red Team (this term refers to teams that conduct security evaluation exercises in an unannounced manner)” to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, critical systems, physical systems, and security controls. People who work on the system every day have great insight into the vulnerabilities of your critical network and should be consulted when identifying potential attack scenarios and possible consequences. Also, ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organisation. Feed information resulting from the “Red Team” evaluation into risk management processes to assess the information and establish appropriate protection strategies.

The following steps focus on management actions to establish an effective cyber security program:

C.2.12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users:

Organisation personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish cyber security organisational structures that define roles and responsibilities and clearly identify how cyber security issues are escalated and who is notified in an emergency.

C.2.13 Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection:

Develop and document robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organisations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

C.2.14 Establish a rigorous, ongoing risk management process:

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management.

C.2.15 Establish a network protection strategy based on the principle of defence-in-depth:

A fundamental principle that must be part of any network protection strategy is defence-in-depth. Defence-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single points of failure must be avoided, and cyber security defence must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

C.2.16 Clearly identify cyber security requirements:

Organisations need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. Formalized policies and procedures are typically used to establish and institutionalise a cyber-security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organisation and eliminates sole dependence on individual initiative. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber-security incident and promote efficient and effective actions during a time of crisis. As part of identifying cyber security requirements, include user agreements and notification and warning banners. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary.

C.2.17 Establish effective configuration management processes:

A fundamental management process needed to maintain a secure network is configuration management. Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

C.2.18 Conduct routine self-assessments:

Robust performance evaluation processes are needed to provide organisations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organisation is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organisational and individual performance.

C.2.19 Establish system backups and disaster recovery plans:

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber-attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

C.2.20 Senior organisational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance:

Effective cyber security performance requires commitment and leadership from senior managers in the organisation. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organisation. It is also essential that senior organisational leadership establish a structure for implementation of a cyber-security program. This structure will promote consistent implementation and the ability to sustain a strong cyber security program. It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

C.2.21. Establish policies and conduct training to minimize the likelihood that organisational personnel will inadvertently disclose sensitive information regarding critical system design, operations, or security controls:

Release data related to the critical network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. “Social engineering,” the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/network is. Never divulge data related to a critical network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfilment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

C.3.0 Guidelines on Crisis Management plan for critical networks:

C.3.1 Strategic issues in crisis management and business continuity:

- Implementation of appropriate measures to reduce the likelihood of incidents occurring and/or reduce the potential effects of those incidents.
- Taking due account of the resilience and mitigation measures
- Providing continuity for critical services during and following an incident
- Taking into account those activities that have not been identified as critical

The effectiveness of above actions depends on a range of factors such as:

- The maximum tolerable period of disruption of a critical activity
- The costs of implementing a strategy and
- Consequences of inaction

C.3.2 Effective crisis management and business continuity strategies also cover the following:

C.3.2.1 People:

Organisations should identify appropriate strategies for maintaining core skills and knowledge. This analysis should go beyond employees to contractors and other stakeholders who posses extensive specialist skills and knowledge. Strategies to protect or provide those skills might include:

- Documentation of the way in which critical activities are performed
- Multi-skill training of staff and contractors
- Separation of core skills to reduce the concentration of risk
- Use of third parties
- Succession planning and
- Knowledge retention and management

C.3.2.2 Premises:

Organisations should devise a strategy for reducing impact of unavailability of its normal work site(s). This may include one or more of the following:

- Alternative premises (locations) within the organisation including displacement of other activities.
- Alternative sites provided by other organisations
- Alternative premises provided by third party specialists
- Working from home or at remote sites
- Other agreed suitable premises and
- Use of an alternative workforce in an established site

C.3.2.3 Technology:

Technology strategies depend on the nature of the technology employed and its relationship with critical activities, but will typically be one or a combination of the following:

- Provision made within the organisation
- Services delivered to the organisation and
- Services provided externally by a third party

Technology strategies may include:

- Geographical spread of technology
- Holding older equipment as emergency replacement or spares and ‘

- Additional risk mitigation for unique or long lead time equipment

Information technology (IT) services require complex continuity strategies. In such cases, consideration should be given to:

- Recovery time objectives (RTO) for systems and applications that support the key activities identified in the business impact analysis.
- Location and distance between technology sites

Number of technology sites

- Remote access
- Use of un-staffed sites as opposed to staffed sites
- Telecom connectivity and redundant routing
- The nature of fail-over (whether manual intervention is required to activate alternative IT provision or it can be done automatically)
- Third party connectivity and external links

C.3.2.4 Information:

Information strategies should be such as to ensure that information vital to the organisation's operation is protected and recoverable according to the time frames prescribed with the business impact analysis. These strategies should include information in both hard copy formats and electronic formats. Any information required for enabling the delivery of organisation's critical activities should have appropriate:

- Confidentiality
- Integrity
- Availability and
- Currency

Appendix - D

Information Security Management System (ISMS)

D.1.0 Information Security and Management:

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organisation are met.

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information of an organisation so that it remains secure. It encompasses people, processes and IT systems.

D.1.1 Information Security Standards:

International Organisation for Standards (ISO) has published the following standards to enable organizations to establish and implement ISMS effectively:

ISO 27002 - Code of Practice for Information Security Controls
ISO 27001 - Information Security Management Systems - Requirements

These standards codify industry experience and security best practices, and are applicable to all types of organizations, irrespective of their size or business.

ISO 27002 is a guidance standard and provides detailed advice on the nature and implementation of security controls for an effective ISMS. This standard covers guidance on managerial, technical and operational aspects of security controls of ISMS.

ISO 27001 is a standard that allows organisations to benchmark their ISMS and check its compliance status through an independent third party audit leading to certification. The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

(a) Understanding an organisation’s information security requirements and the need to establish policy and objectives for information security;

(b) Implementing and operating controls to manage an organisation's information security risks in the context of the organisation’s overall business risks;

(c) Monitoring and reviewing the performance and effectiveness of the ISMS; and

(d) Continual improvement based on objective measurement.

This Standard provides a robust model for implementing the principles governing risk assessment, security design and implementation, security management and reassessment.

D.2.0 Implementing an ISMS:

The following steps will help an organisation in implementing ISMS:

Step-1: Undertaking comprehensive Security Audit to discover the gaps with respect to security best practices as per ISO 27001 standard. CERT-In has created a panel of IT Security auditors that can provide IT security-auditing services on commercial basis. The list of auditors is available on CERT-In website www.cert-in.org.in .

Step-2: Implementing corrective actions to close all gaps. This process can be undertaken internally or with the help of the CERT-In's panel of IT Security Auditors to derive necessary hand holding support to implement the corrective actions. While doing so, use of same agency that was involved in Step-1 to be avoided, in view of potential conflict of interest.

Step-3: Obtaining independent third party endorsement. For this purpose, the services of an independent accredited third party ISMS certification agency may be taken.

D.3.0 Recommended ISMS best practices:

An effective ISMS includes:

- **Risk Assessment and Management -** Conducting periodic IT security risk assessments and determination of acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organisational goals/objectives.
- **Policies and Procedures** – Preparing security policies and procedures in line with the international standard ISO 27001, addressing all aspects of managerial, technical and operational security controls. The following are some examples of security controls:
  - Conduct periodic backup of files critical to mission accomplishment.
  - Storage of back up files should be isolated from any network and physically separated from the originating facility.
  - Ensure procedures are in place that assures the appropriate physical and technical protection of the back up and restoration hardware, firmware and software, such as router tables, compilers and other security-related system software are done in a secure and verifiable manner.
  - Ensure remote access for privileged functions (i.e., access to system control, monitoring or administrative) is permitted only for compelling operational needs and establish strict controls.

  - Ensure remote access to user functions is mediated through a managed access control point (e.g., remote access server in DMZ).
  - Ensure Internet access for networks handling public information is permitted from a secured DMZ (Demilitarized Zone)

- **Security Plans** – Establishing detailed plans for securing networks, facilities, information systems, or groups of information systems, as appropriate (For ex. Patch management, virus protection etc);
- **Security Awareness Training** - Informing personnel about the information security risks associated with their activities and their responsibilities in complying with organisational policies and procedures that are designed to reduce these risks;
- **Periodic Testing and Evaluation –** Periodically testing and evaluating the adequacy and effectiveness of technical security control measures implemented for IT systems and networks on an annual basis and after each significant change to the IT applications/systems/networks. This can include Penetration Testing, Vulnerability Assessment, Application Security Testing and Web Security Testing;
- **Independent Security Audits –** Engaging an independent IT Security auditing organisation to carry out Audit of ISMS on an annual basis;
- **Incident Management** – Establishing procedures for detecting, and responding to security incidents and reporting to CERT-In;
- **Business Continuity and Disaster Recovery** – Developing and continuously updating plans and procedures to ensure continuity of critical operations and recovery within a reasonable time frame.

Appendix – E

Sample Business Impact Analysis (BIA) as applied to a small organization/field office

In this example, an agency maintains a small field office with a local area network (LAN) that supports about 50 users. The office relies on the LAN and its components for standard automated processes, such as developing and using spreadsheets, word processing, and electronic mail (e-mail). The office also maintains a customized database application that supports Inventory, a key resource management process. The network manager is responsible for developing a LAN contingency plan and begins with the business impact analysis (BIA). The LAN includes the following components:

- Authentication/network operating system server
- Database server (supports customized Inventory database application)
- File server (stores general, non-Inventory files)
- Application server (supports office automation software)
- Networked printer
- E-mail server and application
- 50 desktop computers
- Five hubs.

The Contingency Planning Coordinator begins the BIA process by identifying the network stakeholders. In this case, the coordinator identifies and consults with the following individuals:

- Field office manager
- Inventory process manager
- Sampling of network users
- System administrators for each network server

Based on the information gathered in discussions with stakeholders, the Contingency Planning Coordinator follows the three-step BIA process to identify critical information technology (IT) resources, identify outage impacts and allowable outage times, and develop recovery priorities.

Identify Critical IT Resources:

The manager identifies the following resources as critical, meaning that they support critical business processes:

- Authentication/network operating system server (required for users to have LAN access)
- Database server (required to process the Inventory system)
- E-mail server and application
- Five desktop computers (to support five Inventory users)

- One hub (to support five Inventory users)
- Network cabling
- Electric power
- Heating, ventilation, and air conditioning (HVAC)
- Physical security
- Facility.

Identify Outage Impacts and allowable Outage Times:

Next, the manager determines outage impacts and allowable outage times for the critical resources:

Resource	**Outage Impact**	**Allowable Outage Time**
Authentication server	Users could not access Inventory system	8 hours
Database server	Users could not access Inventory system	8 hours
E-mail server	Users could not send e-mail	2 days
5 desktop computers	Users could not access Inventory system	8 hours
Hub	Users could not access Inventory system	8 hours
Network cabling	Users could not access Inventory system	8 hours
Electric power	Users could not access Inventory system	8 hours
Printer	Users could not produce Inventory reports	4 days

Develop Recovery Priorities

Using the table completed in the previous step, the Contingency Planning Coordinator develops recovery priorities for the system resources. The manager uses a simple high, medium, low scale to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

Resource	**Recovery Priority**
Authentication server	High
Database server	High
5 desktop computers	High
1 hub	High
Network cabling	High
Electric power	High
E-mail server	Medium
Printer	Medium
Remaining desktop computers (45)	Low
Remaining hubs (4)	Low

Having completed the BIA, the Contingency Planning Coordinator may use the recovery priority information above to develop strategies that enable all system resources to be recovered within their respective allowable outage times and in a prioritized manner.

A template for completing the BIA is provided below

Business Impact Analysis (BIA) Template:

This sample template is designed to assist the user in performing a BIA on an IT system. The BIA is an essential step in developing the IT contingency plan. The template is meant only as a basic guide and may not apply to all systems. The user may modify this template or the general BIA approach as required to best accommodate the specific system.

Preliminary System Information Organization: Date BIA Completed:

System Name: BIA POC:

System Manager Point of Contact (POC):

System Description: {Discussion of the system purpose and architecture, including system diagrams}

A. Identify System POCs Role:

Internal POC {Identify the individuals, positions, or offices within your organization that depend on or support the system; also specify their relationship to the system}

- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx

External POC {Identify the individuals, positions, or offices outside your organization that depend on or support the system; also specify their relationship to the system}

- xxxx
- xxxx
- xxxx
- xxxx
- xxxx
- xxxx

B. Identify System Resources {Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}

Hardware

- xxxx
- xxxx
- xxxx

Software

- xxxx
- xxxx
- xxxx

Other resources

- xxxx
- xxxx
- xxxx

C. Identify critical roles {List the roles identified in Section A that are deemed critical}

- xxxx
- xxxx
- xxxx

D. Link critical roles to critical resources {Identify the IT resources needed to accomplish the roles listed in Section C}

Critical Role	**Critical Resources**
• xxxx	
• xxxx	
• xxxx	

E. Identify outage impacts and allowable outage times {Characterize the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted}

Resource	**Outage Impact**	**Allowable Outage Time**
	• xxxx	• xxxx
	• xxxx	• xxxx
	• xxxx	• xxxx
		• xxxx
	• xxxx	• xxxx
	• xxxx	• xxxx
	• xxxx	
	• xxxx	• xxxx
	• xxxx	• xxxx
	• xxxx	• xxxx

F. Prioritize resource recovery {List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale (e.g., high/medium/low, 1-5, A/B/C)}

Resource	**Recovery Priority**

Appendix - F

IT Contingency Plan template for use by Critical Sector organizations

F.1. INTRODUCTION:

F.1.1 PURPOSE:

This {system name} Contingency Plan establishes procedures to recover the {system name} following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

  – Notification/Activation phase to detect and assess damage and to activate the plan

  – Recovery phase to restore temporary IT operations and recover damage done to the original system

  – Reconstitution phase to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out {system name} processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated {Organization name} personnel and provide guidance for recovering {system name} during prolonged periods of interruption to normal operations.
- Ensure coordination with other {Organization name} staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

F.1.2 APPLICABILITY:

The {system name} Contingency Plan applies to the functions, operations, and resources necessary to restore and resume {Organization name}'s {system name} operations as it is installed at primary location name, City, State. The {system name} Contingency Plan applies to {Organization name} and all other persons associated with {system name} as identified under Section 2.3, Responsibilities.

The {system name} Contingency Plan is supported by plan name, which provides the purpose of plan. Procedures outlined in this plan are coordinated with and support the plan name, which provides purpose of plan.

F.1.3 SCOPE:

F.1.3.1 Planning Principles:

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- The {Organization name}'s facility in City, State, is inaccessible; therefore, {Organization name} is unable to perform {system name} processing for the Department.
- A valid contract exists with the alternate site that designates that site in City, State, as the {Organization name}'s alternate operating facility.
- {Organization name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency situation that prevents access to the original facility.
- The designated computer system at the alternate site has been configured to begin processing {system name} information.
- The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

F.1.3.2 Assumptions:

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

- The {system name} is inoperable at the {Organization name} computer center and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {System name} hardware and software at the {Organization name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

F.1.4 REFERENCES/REQUIREMENTS:

This {system name} Contingency Plan complies with the {Organization name}'s IT contingency planning policy as follows:

> The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The {system name} Contingency Plan is in line with the following National policies:

- *National Cyber Security Strategy, DeitY Govt. of India*
- *National Information Security Policy, Version 1, May 06*
- *Crisis management Plan for countering cyber-attacks and cyber terrorism*

F.1.5 RECORD OF CHANGES:

Modifications made to this plan since the last printing are as follows: **Record of Changes**

Page No.	**Change Comment**	**Date of Change**	**Signature**

Xxxxxxxxxxxxxxxxxxx xxxxxxxxxxxx

xxx

F.2. CONCEPT OF OPERATIONS

F.2.1 SYSTEM DESCRIPTION AND ARCHITECTURE:

<Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as back up procedures.>

F.2.2 LINE OF SUCCESSION:

The {organization name} sets forth an order of succession, in coordination with the order set forth by the department to ensure that decision-making authority for the {system name} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {organization name} is responsible for ensuring the safety of personnel and the execution of procedures documented within this {system name} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. Continue description of succession as applicable.

F.2.3 RESPONSIBILITIES:

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering {system name} operations.

- The {team name} is responsible for recovery of the {system name} computer environment and all applications. Members of the team name include personnel who are also responsible for the daily operations and maintenance of {system name}. The team leader {title} directs the {team name}.
- [Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation]

<Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.>

The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure XX below.

[Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel]

F.3. NOTIFICATION AND ACTIVATION PHASE:

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {system name}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

In an emergency, the {Organization name}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in *Annexure II.* The notification sequence is listed below:

- The first responder is to notify the Contingency Planning Coordinator. All known information must be relayed to the Contingency Planning Coordinator.
- The systems manager is to contact the Damage Assessment Team Leader and inform them of the event. The Contingency Planning Coordinator is to instruct the Team Leader to begin assessment procedures.
- The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the Damage Assessment Team is to follow the outline below.

Damage Assessment Procedures:

- (Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)
- Upon notification from the Contingency Planning Coordinator, the Damage Assessment Team Leader is to …
- The Damage Assessment Team is to ….

Alternate Assessment Procedures:

- Upon notification from the Contingency Planning Coordinator, the Damage Assessment Team Leader is to …
- The Damage Assessment Team is to ….
    - When damage assessment has been completed, the Damage Assessment Team Leader is to notify the Contingency Planning Coordinator of the results.
    - The Contingency Planning Coordinator is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
    - Based on assessment results, the Contingency Planning Coordinator is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. {System name} will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. Other criteria, as appropriate.

- If the plan is to be activated, the Contingency Planning Coordinator is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the Contingency Planning Coordinator, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The Contingency Planning Coordinator is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The Contingency Planning Coordinator is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the Organization's arrival.
- The Contingency Planning Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

F.4. RECOVERY OPERATIONS:

This Section provides procedures for recovering the application at the alternate site, whereas, other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the {system name} at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations:

Recovery Goal. State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, State the team names and list their respective procedures.

- {team name}

  – Team Recovery Procedures
- {team name}

  – Team Recovery Procedures
- {team name}

  – Team Recovery Procedures

Recovery Goal. State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, State the team names and list their respective procedures.

- {team name}

  – Team Recovery Procedures
- {team name}

  – Team Recovery Procedures
- {team name}

  – Team Recovery Procedures

Recovery Goal. [State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, State the team names and list their respective procedures.]

F.5. RETURN TO NORMAL OPERATIONS:

This Section discusses activities necessary for restoring {system name} operations at the {Organization name}'s original or new site. When the computer center at the original or new site has been restored, {system name} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration:

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- {team name}
  – Team Resumption Procedures
- {team name}
  `– Team Resumption Procedures

F.5.1 CONCURRENT PROCESSING:

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- {team name}
  – Team Resumption Procedures
- {team name}
  – Team Resumption Procedures

F.5.2 PLAN DEACTIVATION:

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. Materials, equipment, and back up media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- {team name}
  – Team Testing Procedures
- {team name}
  – Team Testing Procedures

F.6. PLAN APPENDICES:

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Business Continuity Plan.

Appendix – G

G.1. Control Room Details of CERT-In / CERT - O

Primary Contact - CERT-In		
Name	**Designation**	**Contact Details**
Dr Gulshan Rai	Director	Tel. Nos : Off: 011-24368544 Res: 011-22323085 FAX: 011-24366806 Mobile: 9810643244 Email: grai@cert-in.org.in grai@mit.gov.in

Alternate Contact - CERT-In		
Name	**Designation**	**Contact Details**
Shri Anil Sagar	Operations Manager	Tel. Nos: Off: 011-24368579 FAX: 011-24368579 Mobile: 9810874430 Email: anil@cert-in.org.in anil@mit.gov.in

Incident Response Help Desk - CERT-In
Tel. Nos: (Toll free) : 1800-11-4949 Tel No: 011-24368572 FAX: (Toll free) : 1800-11-6969 FAX: 011-24368546 Email: incident@cert-in.org.in info@cert-in.org.in

Primary Contact - CERT- O		
Name	**Designation**	**Contact Details**

Alternate Contact - CERT-O		
Name	**Designation**	**Contact Details**

Incident Response Help Desk - CERT- O

G.2. Incident Reporting Procedures:

Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents.

By reporting such computer security incidents to CERT-O/CERT-In, the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-O/CERT-In to correlate the incidents thus reported and analyse them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

G.2.1 Reporting of an incident:

System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-O/CERT-In. They may use the following channels to report the incident.

Contact information of CERT-In
Email: incident@cert-in.org.in
Helpdesk: +91-1800-11-4949 (Toll Free) Fax : +91-1800-11-6969 (Toll Free)

Contact information of CERT-O
Email:
Helpdesk: +91- (Toll Free) Fax: +91- (Toll Free)

G.2.2 Contents of Incident Report:

The following information (as much as possible) may be given while reporting the incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

For details please refer the incident reporting form given in Para. 2.6.

G.2.3 Verification:

CERT-O/ CERT-In will verify the authenticity of the report.

G.2.4 Triage:

CERT-O/ CERT-In will then analyse the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. CERT-O will designate a team as needed.

G.2.5 Incident Response:

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:—

- Identification: to determine whether an incident has occurred, if so analysing the nature of such incident, identification and protection of evidence and reporting of the same.
- Containment: to limit the scope of the incident quickly and minimise the damage
- Eradication: to remove the cause of the incident
- Recovery: taking steps to restore normal operation

CERT-O/ CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice. CERT-O/ CERT-In will not physically deploy or send any member for attending the incident response activity at the site of occurrence. The priority of assisting in responding to the incidents will be decided by CERT-O/ CERT-In keeping in view the severity of incident and availability of resources.

G.2.6 Incident Reporting Form:

<table>
<tr><td colspan="4"><b>Form to report Incidents to CERT-In/CERT-O</b></td></tr>
<tr><td colspan="2">For official use only:</td><td colspan="2">Incident Tracking Number : <b>CERT-In/O-xxxxx</b></td></tr>
<tr><td colspan="4">1. Contact Information for this Incident:</td></tr>
<tr><td>Name:</td><td colspan="2">Organisation:</td><td>Title:</td></tr>
<tr><td>Phone / Fax No:</td><td colspan="2">Mobile:</td><td>Email:</td></tr>
<tr><td colspan="4"><b>Address:</b></td></tr>
<tr><td colspan="4">2. Sector : (Please tick the appropriate choices)</td></tr>
<tr><td>□ Government
□ Financial
□ Power</td><td>□ Transportation
□ Manufacturing
□ Health</td><td>□ Telecommunications
□ Academia
□ Petroleum</td><td>□ InfoTech
□ Other ___________</td></tr>
</table>

3. Physical Location of Affected Computer/ Network and name of ISP.

4. Date and Time Incident Occurred:

Date:	Time:

5. Is the affected system/network critical to the ehavior ion’s mission? (Yes / No). Details.

6. Information of Affected System:

IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model

7. Type of Incident:

□ Phishing

□ Network scanning /Probing

□ Break-in/Root Compromise

□ Virus/Malicious Code

□ Website Defacement

□ System Misuse

□ Spam

□ Bot/Botnet

□ Email Spoofing

□ Denial of Service(DoS)

□ Distributed Denial of Service(DdoS)

□ User Account Compromise

□ Website Intrusion
□ Social Engineering

□ Technical Vulnerability
□ IP Spoofing

□ Other________________

8. Description of Incident:

9. Unusual ehavior/symptoms (Tick the symptoms)

□ System crashes
□ New user accounts/ Accounting discrepancies
□ Failed or successful social engineering attempts
□ Unexplained, poor system performance
□ Unaccounted for changes in the DNS tables, router rules, or firewall rules
□ Unexplained elevation or use of privileges
□ Operation of a program or sniffer device to capture network traffic;
□ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
□ A system alarm or similar indication from an intrusion detection tool
□ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server

□ Anomalies
□ Suspicious probes
□ Suspicious browsing
□ New files
□ Changes in file lengths or dates
□ Attempts to write to system
□ Data modification or deletion
□ Denial of service
□ Door knob rattling
□ Unusual time of usage
□ Unusual usage patterns
□ Unusual log file entries
□ Presence of new setuid or setgid files
□ Changes in system directories and files
□ Presence of cracking utilities
□ Activity during non-working hours or holidays
□ Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.

11. Agencies notified?

□ Law Enforcement	□ Private Agency	□ Affected Product Vendor	□ Other________________

12. When and How was the incident detected:

13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)

□ Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION

14. IP Address of Apparent or Suspected Source:

Source IP address:	Other information available:

15. Security Infrastructure in place:

	Name	OS	Version/Release	Last Patched/Updated
(1)	(2)	(3)	(4)	(5)
Name OS Version/Release Last Patched / Updated				
Anti-Virus				

(1)	(2)	(3)	(4)	(5)
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected

□ 1 to 10

□ 10 to 100

□ More than 100

17. Actions taken to mitigate the intrusion/attack:

□ No action taken

□ System Binaries checked

□ Log Files examined

□ System(s) disconnected form network.

□ Restored with a good backup

□ Other____________________

Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident.

Mail/Fax this Form to: CERT-In, Electronics Niketan**,** CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in

Mail/Fax this Form to: CERT-O Fax: or email at:

Appendix H

Nature and Severity of crisis, Authorities responsible and steps for mitigation

Severity Level of Crisis	Nature of Crisis	Authorities responsible and Steps for mitigation
Level 1 Response **Scope:** **Individual Organisation**	All attacks	**Responsibility:** ***(Mention name of Affected Organisation)*** **Steps to be taken by the Affected Organisations** **General** • Notify incidents to respective administrative Ministry/Department • Monitor and detect anomalous behaviour and degradation of service in network and systems • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-O/ CERT-In /NTRO/MoD, IDS (DIARA) • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-In and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration *vis-à-vis* ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks mentioned below. • Change all user/root/administrator passwords in all systems and network devices • Install updated software patches on Operating System and all other system software running on computer servers and Personal computers in the network **Mitigation Steps - Specific to nature of cyber-attacks/crisis**
	Virus/Worm/Spyware/ Botnet attacks	• Isolate affected systems/network segments from LAN and Internet • Scan all files in the suspected systems, including emails for viruses. • Clean the affected systems with the updated antivirus software. • Install updated Antivirus/anti-spyware on all systems (servers and Personal Computers)
	DoS/DDoS attacks	• Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack such as flooding of particular types of packets/requests • Allocate traffic to unaffected available network paths, if possible, to continue the services • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP

		• Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Install updated software patches on all the network devices such as Routers, Firewalls, IDS, IPS and switches.
	High Energy RF-based DoS Attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio or the increased noise levels in the airwaves. • Identify the other devices due to which RF interference occurs and physically remove them. • Deploy IPS/IDS to detect rouge access points
	DNS Attack	• Check for version updates at the DNS server and install latest software patches • Implement spoofing countermeasures • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Adopt source IP address verification • Implement DNSSec
	Attack attempts/scans on Servers, Routers, Firewall etc.	• Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required. • Check the logs of these devices for source of attack.
	Phishing attacks	• Keep watch on phishing sites • Alert customers regarding the known phishing sites • Encourage customers to use anti-phishing enabled browsers • Shutdown phishing sites in coordination with concerned ISP and CERT-In/CERT-O
	Mail Server attacks	• Deploy hot standby mail servers in physically separated networks and places which can be made operational when the main server is attacked • Disable all other ports and services on mail servers • Enforce strong password policy and encourage users to change passwords periodically
		On report of the incident, CERT-In /CERT-O would take following supportive actions— • Analyse the information/logs received from affected organisations. • Check for latest patches/updates from various sources including vendors • Consult the vendors and other sources to help the organisations in resolving the problems • Document the vulnerability information and disseminate • In case of phishing attacks, take appropriate action to block the phishing sites by interfacing with concerned organisations, ISPs and international CERTs • In case of Botnet attacks, locate Command & Control server and initiate action to disable the same in coordination with ISPs

Level 2 Response **Scope:** **Multiple Organisations**	All attacks	**Responsibility:** ***(Mention Name of Respective Department of the State)*** **Steps to be taken by affected Organisations** **General** • Notify incidents to respective administrative Ministry/Department • Monitor and detect anomalous behaviour and degradation of service in network and systems • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In/CERT-O /NTRO/MoD, IDS (DIARA) • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-In/CERT-O and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration *vis-à-vis* ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks mentioned below. • Change all user/root/administrator passwords in all systems and network devices
		Mitigation Steps - Specific to nature of cyber-attacks/crisis
	Virus/Worm/Spyware/Botnet attacks	• Isolate affected systems/network segments from LAN/Internet • Scan all files in the suspected systems, including emails for viruses • Install Antivirus/anti-spyware updates • Clean the affected systems with the updated antivirus software • Block the infection/attack vectors through IPS/Firewall
	DoS/DDoS attacks	• Shift critical services to alternate channels. • Incase of IP based attacks, shift hosting of affected services to different ISPs. • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends • Install updated patches on the network devices
	High Energy RF-based DoS Attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio or the increased noise levels in the airwaves. • Identify the other devices due to which RF interference

		occurs and physically remove them. • Relocate the Access Points incase of Wireless Networks
	DNS Attack	• Change the preferred DNS server • Implement Source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Run separate DELEGATED and RESOLVING name servers • Disable Recursion on DNS server authoritative for the zone • Restrict zone transfers to slave name servers and other authorized software • Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. • Check for version updates at the DNS server and install latest patches • Implement split DNS architecture • Implement anycast technology on DNS server
	Attacks on Servers, Routers, Firewall etc.	• Check for the effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required. • Replace compromised systems with trusted ones. • Check for version updates/patches and install latest patches for routers, firewall and IPS • Check the logs of these devices for source of attack
	Mail server attacks	• Activate hot standby mail servers and direct mail traffic appropriately.
		On report of the incident, CERT-In / CERT-O would take following supportive actions— • Analyse and correlate the information/logs received from affected organisations • Check for latest patches/updates of system software, network devices and antivirus signatures from vendors and other sources • Consult the vendors and other sources to help the organisations in resolving the problems • Contact the concerned CERTs or ISPs from where the attacks are originating for blocking in case of DoS/DDoS attacks Document the resultant vulnerability, prepare vulnerability notes and disseminate to cyber community.
Level 3 Response **Scope:** **State/** **Multiple States**		**Responsibility:** **(Mention Name of Respective Department of the State)** • Notify the incidents to SCMC/NCMC, as the case may be • Depending upon the situation request for the meeting of SCMC/NCMC

	All attacks	**Steps to be taken by affected Organisations** • Notify incidents to respective administrative Ministry/Department • Implement the Contingency Plan • Deploy onsite response team on 24X7 basis • Limit the access to systems and networks from outside in consultation with concerned ISPs. • Enable hot stand-by systems/servers with alternate Traffic paths. • Take all logs (system, application, security, access, error etc.) of affected systems and data therein and keep them separately for analysis and forensics • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration *vis-à-vis* ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks in level 1 & 2. • Carry out file integrity checks on all the systems • Restore systems from trusted back-ups and validate the systems and networks before connecting to Internet. • Change all user/root/administrator passwords in all systems and network devices
		Actions to be undertaken by CERT-In/ CERT-O • Analyse the on-going attacks/traffic and seek assistance from Vendors and other CERTs if required • Work closely with affected organisations, ISPs and other agencies to provide all necessary help to mitigate the incident. • Advise appropriate measures to isolate systems/networks at organisations/regions.
Level 4 Response **Scope:** **Entire Nation**	All attacks	**Responsibility:** **(Mention Name of Respective Department of the State)** • Notify the incidents to NCMC • Request for the meeting of NCMC **Steps to be taken by affected Organisations** • Carry out all the steps indicated in level 3 • Implement directives of NCMC, respective administrative Ministry/Department • Implement specific advisories and instructions issued by CERT-In / CERT-O and other designated agencies.
		Actions to be undertaken by CERT-In/ CERT-O • Analyse the on-going attacks/traffic and seek assistance from Vendors and other CERTs if required • Work closely with affected organisations, ISPs and other agencies to provide all necessary help to mitigate the incident. • Advise appropriate measures to isolate systems/networks at organisations/regions.

Appendix I

Cyber Resilience Control matrix:

Building cyber resilience begins with effective protection of five key components within any system (i.e. key information and technology assets) – the user identity, system processes, data and hardware & software platform along with network of connections between systems. These components are defined as follows:—

Identity: The representation of a user or organization within a system.

System Processes: The actual programs running within the system that may be executing on behalf of user or at root level within the operating system.

Hardware & Software Platform: Typically this will be a physical manifestation of the system as hardware and software, but it may also be a virtualized platform residing on a cloud infrastructure or in the data centre. The information security management system (ISMS) Risk Assessment Methodology and Procedures & controls for State Data Centre based on ISO 27001:2005 may be referred at *http://deity.gov.in/content/data-centre.*

Data: The data either physically stored or held in memory within the system.

Network: The communication link between systems and all the protocols for establishing and securing that communication. Commonly, the gateways on the network act as enforced barriers to communication that may act as a boundary or filter to prevent some communications while enabling others such as network firewall.

Achieving cyber resilience is about understanding the sensitivity and interdependency of critical assets and selecting appropriate technical controls for protection, detection, containment and recovery from cyber disruptive activities and assigning resilience rating for each system component by the organization depending on the services provided by them and their respective Service level Agreements (SLA).

Cyber resilience components & control matrix

Component	Protect	Detect	Contain	Recover
Identity	• Controlled access based on need-to-know • Enforce Strong password policy • Multi factor authentication • Usage of Digital Certificates	• Maintenance and Analysis of complete security events and audit logs • Privilege escalation monitoring and alerting	• Minimize the invalid logon counts • Revocation of digital certificate • Change access control on all devices • Continuous account monitoring and deactivating the dormant accounts	• Offline recovery procedures for logging into accounts • Alternative Indicators

System Processes	• Effective Security Patch Updating Mechanism on applications etc. • Following Best Security practices during Software Development Lifecycle • Secure configuration • Malware defenses	• Forensic Memory Analysis • File integrity checking • Malware Analysis	• Policy based restrictions on process actions • Reconfiguration of settings • Usage of Sandbox Security Mechanism	• Assured Data Back-ups • Clustering • Recovery Time Objectives (RTO) for system and support • Manual /automated takeover to activate alternative IT provision • Use of Unstaffed sites as opposed to staffed sites
Hardware and Software Platform	• Asset Inventory (asset classification and management) • Supply chain protections • Regular review of configuration files : OS/middleware • Boot process integrity check	• Continuous vulnerability testing and remediation • Tamper detection mechanism • Platform Security Assessment (Review of System architecture/Operating system configuration/Security management controls/System configuration)	• Remote Wipe on failed logins • Code Integrity Checks to help prevent malicious code from being injected into system files or into the kernel at load/run time	• Baseline remote image deployment • Usage of Virtual environment • Assured Back-up and replication • Replacing compromised files with clean versions
Data	• Database access control : Regular review of access privileges to users of the database/use of biometric technology • Data Encryption while in-process, handling, storage or transit. • Data Masking (for sensitive information)	• Monitoring Data flow to detect data leakage • Forensic disk imaging and analysis • Monitoring remote access • Database integrity Checking	• Application restrictions monitoring • Data Leakage Prevention (system designed to detect potential data leakage while in-process, handling, storage or transit • Access Control on Database	• Assured Data Back-ups and physical segregation of back-up • Storage replication Mirroring/Cloning • Database reprocessing (Going back to a known point of database activity before the problem occurred and reprocessing work from that point forward)

Network	• Limitation and control of ports, protocols and services • Wireless Device Control • Following Best Practices for secure configuration of network devices	• Centralised network log analysis for wired & wireless networks • Honey-net • Network Scanning and Analysis	• Isolation of trusted networks from untrusted networks. • Denial of service offload to ISP and cloud • Reconfiguration of impacted network devices • Modify access control (all user/root/administrator passwords) in all systems and network devices	• Alternate network routing • Alternative cloud communications • Usage of devices in cluster mode/load balancing mode

Appendix - J

IT Security best practices Compliance and Assurance – 'Levels of Assurance'

Sl. No.	Assurance Level	Description	Methods of verification
1	**Level 1 – Assurance of systematic approach to IT Security**	Organisation is aware of IT security best practices and has defined and documented its IT security plan, policies and procedures covering people, products, technology and processes. Evidence in the form of appropriate references to the IT security plan, policies and procedures exists.	• Questionnaire based check-list and • Remote or on-site desk-top assessment of check-list response
2	**Level 2 – Assurance of compliance to IT security best practices**	Organisation has implemented IT security best practices based on clear understanding of risks, threats & vulnerabilities and the compliance has been verified by a self-assessment process or by an independent third party auditing organisation.	Self-assessment report or independent third party audit report
3	**Level 3 – Assurance of an adequate IT security posture**	Organisation has conducted IT security posture verification (by way of security testing of its IT infrastructure involving VA/PT, application security testing, code walk-throughs etc.) by an independent third party auditing organisation.	Security testing of IT infrastructure involving VA/PT, application security testing, code walk-throughs etc and a report is available for the same
	Level 3+ - Assurance of IT security crisis response & ability to resist cyber attacks	Organisation has participated in the cyber security drills to have its IT security crisis response & ability to resist cyber-attacks tested and verified	Cyber security drills results with CERT-In/ CERT-O
4	**Level 4 – Assurance of proactive IT security monitoring and mitigation of threats and vulnerabilities**	Organisation has implemented mechanisms for proactive IT security monitoring and mitigation of threats and vulnerabilities. These mechanisms allow for technology based monitoring and analysis of IT security incidents for proactive preventive actions (Ex. IPS/IDS, SIEM, flow based analysis etc).	Technology based monitoring and analysis (Ex. IPS/IDS, SIEM, flow based analysis etc) evidenced in terms of governance reports and management feedback

	Level 4+ - Assurance of proactive sharing and mitigation of IT security threats & vulnerabilities.	Organisation has implemented mechanisms for proactive sharing and mitigation of IT security threats & vulnerabilities byway of active collaboration with CERT-In,CERT-O, ISACs etc	Collaboration with CERT-In, CERT-O, ISACs etc evidence in terms of communication trail
	Level 4+ + - Assurance of proactive prediction of residual IT security risks & attack paths and mitigation	Organisation has implemented mechanisms for proactive prediction of residual IT security risks & attack paths and mitigation of IT security threats and vulnerabilities.	Attack path analysis

Appendix - K

Table 2.1: Nature of cyber crisis, possible targets and Impact

Type of Crisis	Possible Targets	Related impact
a) **Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure**	• Sensitive State Government's Critical Information infrastructure like Infrastructure at Odisha Data Centres and Odisha State Wide Area Network • Other infrastructures like Routers, Switches, Database and DNS Servers, Web portals	• Pre-cursor to hacking and focused attack leading to cyber crisis • Total/partial disruption of e-Governance, Public and Banking services
b) **Large scale defacement and semantic attacks on websites** • A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website • Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated	• State Government portal ,other portals like SAMS,OPSC, Treasury, commercial tax , e District, e Municipality and other key sites. .	• Huge national embarrassment, loss of image, reputation etc. • Total/partial disruption of services/activities • Dissemination of false/misleading information • Monetary loss, damage to reputation, loss of image etc
c) **Malicious Code attacks (virus/worm/ Trojans / Botnets)** • Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, trojans, spyware, adware and Bots • Sophisticated malware such as Stuxnet targeting	• Large & key state data bases at State Data Centre such as commercial tax information network, citizen data base, Treasury database , CCTNS etc. • Internet Service Provider network /infrastructure • Public access networks	• Hanging of Computer systems • Partial or No response from Computer system • Total/partial corruption of databases • Total/partial break down of data access services • Monetary loss, damage to reputation, loss of image etc • Total/partial corruption of data bases • Total/partial break down of data access services

Industrial Control Systems that are part of networks separated through 'airgap' from regular Internet facing networks		• Monetary loss, damage to reputation, loss of image etc • Total/partial disruption of services/activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc
d) Malware affecting Mobile devices • Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile, Blackberry OS	• Mobile devices using affected Operating System and connected Computer systems	• Unauthorized disclosure of user's data and contact details • Misuse of devices resulting in excessive billing • Theft of sensitive user credentials
e) Large scale SPAM attacks Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems. As a result, spamming could disrupt e-mail services, messaging systems and mobile phone communications.	• ISP networks • Key Govt. networks like OSWAN, Secretariat LAN	• Significant slow down in network performance • Total/partial disruption of E-mail communication services • Severe drain on network resources. • Significant reduction in access to critical network services. • Increased possibility of virus/worm infection

Identity Theft Attacks **f) Large scale spoofing** • Spoofing is an attack aimed at 'Identity theft' o Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage	• High profile users in Government, State PSUs and key economic installations	• Increased possibility of identity theft and root privileges compromise leading to penetration into sensitive IT systems and Databases • Loss of sensitive data, monetary loss and loss of image.
g) Phishing attacks • Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds o Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication • Vishing attacks o Vishing is a combination of 'voice' and 'phishing'. It is the practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. It exploits the trust in landline telephone services and uses VoIP to trick the user.	• Users of State Co-operative Banks, large e-Commerce organizations, key e-Governance entities etc • Generic internet users and their associated ISP networks	• Loss of sensitive personal data, monetary loss and loss of image and trust • Financial frauds • Malware proliferation

• SMSing attacks o These are phishing attacks launched through SMS service via Mobile phones		
h) Social Engineering Art of manipulating people into performing disclosure actions or divulging confidential information	• Individual users such as senior executives & officials, celebrities • Network/System/Database Administrators	• Loss of sensitive personal Data and key information
i) Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks • DoS is an attempt to make a computer resource unavailable to its intended users • A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. • DDoS attacks are launched through a Botnet which is a network of compromised computer systems called 'Bots'	• Public utility services • Fire • Water supply • Hospitals/ Ambulance • Police • Transport • Electricity • Web-based key economic targets such as State undertaking Banks/FIs, online reservations etc	• Total/partial disruption of services for prolonged periods • Failed/aborted missions • Possible damage to life and/or property • Total/partial disruption of services for prolonged periods • Monetary loss, damage to reputation, loss of image etc
j) Domain Name Server (DNS) attacks • Attacks on DNS Servers aim at denying resolution of a domain name into a IP address, reverse DNS queries or redirecting users and traffic to fake/malicious domains in some other country to disrupt internet and mail traffic in the country	• Country level domain registry systems (NIXI ".IN" registry) • International gateway or ISP/ large corporate server systems	• Total/partial disruption of '.in' registry services • Possible damage of/inaccessibility to domain registry database or resolution services • Availability of services (Web sites /applications, mail servers etc.) depending on DNS infrastructure would be impacted causing inconvenience to users • Illegal diversion of Internet and mail traffic to some other countries

		• Total/partial disruption of internet traffic nationally/internationally • Total/partial break down of on line economic activities • Monetary loss, damage to reputation, loss of image etc
k) Application Level Attacks • Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases	• e-Governance - Including large & key state level databases such as Commercial tax information, citizen database, plan information, Treasury, Hospital Information System etc. • Business and Banking Applications - Large & key economic data bases such as banks/FIs, depositors, insurance, data centers, reservations etc -	• Data manipulation which may result in huge economic fallouts including monetary as well as business loss • Total/partial Disruption of services/ data access services • Loss of sensitive data and loss of image & trust • Total/partial corruption of data bases • Dissemination of false/misleading information
l) Infrastructure attacks • Attacks such as DoS, DDoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralised/Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware such as Stuxnet.	• Supervisory Control and Data Acquisition systems (SCADA) and Centralized as well as distributed control systems of power, petroleum, transport, air traffic control, refineries, fertilizers etc and all process industries • International gateways/ISPs • Satellite/under Sea Cables • Data Networks	• Total/partial disruption of services/activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc • Huge economic fallouts including monetary as well as business loss

m) Compound attacks • By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber-attack.	• Public utility services ○ Fire ○ Water supply ○ Hospitals/ Ambulance ○ Police ○ Transport ○ Electricity • Web based economic targets • Large & key national & economic databases • Mission Critical systems • International gateway/ISPs	• Total/partial disruption of services/activities • Significant slow down in disaster/emergency response capabilities that can magnify the impact of a physical attack • Huge economic fallouts including monetary as well as business loss • Damage to reputation, loss of image etc.
n) Router level attacks • Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication	• Gateway/ISP routers • Routers of large & key economic targets such as bank/FI networks, corporate networks etc. • ADSL/Wi-Fi Routers used by small offices/home users	• Total/partial disruption of internet traffic nationally/internationally • Total/partial break down of online economic activities • Huge economic fallouts including monetary as well as business loss • Total/partial break down of online economic activities • Huge economic fallouts including monetary as well as business loss • Possession of Router's control by attackers and re-redirection to malicious websites through rogue DNS Server entries for conducting malicious activities
o) Attacks on Trusted infrastructure Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks. Compromise of	• Certifying Authorities Authentication infrastructures • Secure Communication Protocols and systems • Public Key Infrastructure • SSL Servers	• Blocking of handshaking resulting in disruption of financial and authentication services • Large scale Man-in-the-middle attacks resulting in disclosure sensitive data and user information

infrastructure of Certifying authority or key management systems of product/application owners may result in breakdown of trust of users and misuse of authentication mechanisms (i) Denial of Service attacks (ii) Rogue certificates		• Redirection of users to fake websites with dubious authentication • Signing malicious code to make it appear as legitimate • Large scale cyber espionage
p) High Energy Radio Frequency Attacks Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service	• Wireless Networks ▪ Wi-Fi ▪ Wi-MAX • Mobile Networks • Satellite Network Communication Systems	• Disturbances or total disruption in the Wireless, Mobile and Satellite Networks • Appliances like, phones, Bluetooth and Microwave devices etc. • Some RF Jamming tools may use very high energy sufficient to even break down the electronics and make it to malfunction totally.
q) Cyber Espionage and Advanced Persistent Threats Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware. The data from compromised system is siphoned off to remote locations. Common channel of attacks include spoofed/compromised e-mail accounts of key officials, social networking sites and drive-by-download through watering hole websites.	• Sensitive Government Organizations like Intelligence/Vigilance wing • PSUs/Corporate	• Disclosure of sensitive information • Data theft • Compromise of critical internal systems

Appendix - L

Prevention and Precautionary measures

Responsibility of Chief Information Security Officers (CISO)	Chief Information Security Officers to coordinate the security related issues/implementation across the State as well as coordination and interface with CERT-In and with CERT-O
Responsibility of Addl. Chief Information Security Officers (ACISO)	To assist the CISO to look after day-to-day activities like coordination for Security compliance efforts across the state, coordination with various security agencies like CERT-In, STQC, CERT-O etc..
Responsibility of Information Security Officers(ISO)	Nominated Information Security Officers to coordinate the security related issues/implementation within the organisation as well as coordination and interface with CERT-O, CISO/ACISO and Government of Odisha .
Information Security Policy and Implementation of Best Practices	Every Organisation/Department should formulate suitable Information Security Policy and identify appropriate information security management practices keeping in view their business needs as per Information Security Management System (ISMS) Best Practices standard ISO 27001. The identified practices should be implemented. Organizations should necessarily implement the following steps while implementing the ISMS. • The Information Security Policy should clearly identify the three components namely process, technology and mitigation of incidents. • Undertake comprehensive Risk Assessment of the Information Technology/Network assets. • Implement appropriate security control measures such as those defined in the ISO 27001, which include Service Level Agreements with various service providers. Steps need to be taken for ISMS implementation are given Appendix IV of this document. Where considered necessary, assistance of experts may be taken.

Business Continuity Plan (BCP)	Define Contingency Plan (Business Continuity Plan) to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.
Disaster Recovery Plan (DRP)	Establish Disaster Recovery (DR) Plans with adequate redundancy to take over the operation in case of the need.
Security of Information Infrastructure and Network	• Organizations/Department should secure the entire IT infrastructure including the network by implementing appropriate hardening measures. • Security devices may be installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system. Configuration of these security devices should be checked at the time of installation as well as at the time of significant changes for the needed functionalities and security features. • The security mechanism should include appropriate devices and methods to log and monitor the events to detect network scanning, probing and Reconnaissance attempts on the IT infrastructure. These attempts should be regularly reviewed and analysed for initiating necessary preventive measures. • The remote monitoring and maintenance of the security devices should be strictly restricted to authorized persons only. • The software at network, system and application level should be regularly upgraded by applying/installing upgrades and updates.
Network Traffic Scanning	The network traffic scanning technique provides visibility into the state of the network and identifies deviations from baselines that may indicate abnormal or suspicious behaviour. The traffic patterns provides leads on the targeted ports such as 80, 25, 23 which gives leads to the attack targeted on the services like ‘http’, ‘smtp’, ‘ftp’ or spread of malicious code like ‘Bots’. For example, if it is observed that suddenly there is rise on the port 25, associated with e-mail service; this may indicate that e-mail based worm is spreading at a high speed. A sudden traffic rise on the

	IRC ports may indicate surge in the ‘Botnet activity’. The network traffic flows thus gives the exact portrait of the communications happening on the network, irrespective of their state whether a normal or an anomaly. Majority of attacks such as Distributed Denial of Service (DDoS), Worm, Spyware, Botnet detection, malicious scan of any nature etc. at the organisation level could thus be detected by analyzing network flow-data traffic. Industry solutions are available to collect and analyze network flow traffic on the gateway routers and switches. Network flow data DO NOT contain any content data and is totally non-intrusive on the network. The organisations may use network flow data for security analysis to detect attacks onto the networks.
Isolation of critical networks	The critical networks should be isolated from other production networks connected over intranet/Internet. At no point of time the gap between critical network and production network over intranet/internet be compromised. No transfer of data from a intranet/internet based network to a critical network or *vice versa* be allowed. In case required, it should be under strict control and thoroughly screened. There are malicious codes specifically designed to target critical infrastructure systems by means of spreading through systems connected over internet. Risk assessment and regular monitoring of critical networks is essential for security of critical infrastructure.
Implementation of Security Guidelines issued by Nodal Ministry and agencies like CERT-In	Organisations should implement Security Guidelines and advisories both with respect to cyber and physical security issued by respective nodal Ministry and CERT-In from time to time.
Manpower engaged in cyber security activities	**Screening and background checks** Background verification checks on all employees engaged in implementing and monitoring cyber security and crisis management plan, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the requirements of task and

	responsibilities, the classification of the information to be accessed, and the perceived risks. Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:— a) availability of satisfactory character references, e.g. one business and one personal; b) a check (for completeness and accuracy) of the applicant's *curriculum vitae*; c) confirmation of claimed academic and professional qualifications; d) independent identity check (passport or similar document); and e) more detailed checks, such as credit checks or checks of criminal records. Information security management practices based on ISO 27001 standard provide guidance with regard to screening and background checks in respect of employees and other personnel. The organisation may consider following ISO 27001 best practices. **Roles and responsibilities:** Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy. Security roles and responsibilities should include the requirement to: a) implement and act in accordance with the organisation's information security policies; b) protect assets from unauthorized access, disclosure, modification, destruction or interference; c) execute particular security processes or activities; d) ensure responsibility is assigned to the individual for actions taken; and e) report security events or potential events or other security risks to the organisation.

	Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process. Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organisation's employment process, e.g. engaged via a third party organisation, should also be clearly defined and communicated. *Incident response matrix in* ***Appendix B*** *of this document indicate the roles and responsibilities of various personnel engaged in incident response activities.*
Audit and Assurance	• Organisations should undertake comprehensive security audit of the entire IT infrastructure including Local Area Network and Wide Area Network by independent auditor to discover the gaps with respect to best security practices and take appropriate corrective actions. A panel of IT security auditors who provide IT security audit is available on CERT-In website www.cert-in.org.in. • The audit of the system should be undertaken at least once in a year and also as and when any significant addition or alteration in respect of hardware, software, network resources, policies and configurations of systems and sub systems are affected. • Following the audit, compliance with the security policy should be documented in the annual report.
Security Training and Awareness	All employees of the organization/Department and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function. Awareness training should commence with a formal induction process designed to introduce the organisation's security policies and expectations before access to information or services is granted.

	Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. • Latest Technologies and threats • Implementation of Security Policy • Physical Security Procedures • Access Control Procedures • Use of Licensed Software Packages • Malicious code and Botnets and their prevention • Reporting and mitigation of incidents • Cyber Crisis Management The security awareness, education, and training activities should be suitable and relevant to the person’s role, responsibilities and skills. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.
Sharing of Information pertaining to incidents	All organizations should provide and share all information pertaining to cyber security incidents with CERT-In and other designated agencies.

Appendix - M

Cyber security emergency – Levels of concern

The table outlines the threat levels, spread of attack and related conditions that become the basis for declaration of a crisis. The table also outlines the crisis/contingency affecting the systems of individual organisation, multiple organisations, states and nation leading to crisis of different levels. The levels of crisis are interrelated. Each subsequent level will follow preceding one. No level other than level 1 will come in isolation:

Threat Level	Condition
Level 1 **Guarded** **Scope: Individual Organisation**	Perceptible change/variation in system performance and discovery of critical/non critical vulnerabilities/exploits and attacks that can affect normal operation of network and IT systems of individual organisation such as: • Visible signs of viruses/worms/ Bots/malware/Keyloggers/Spyware • Spam • Identity theft (Phishing, spoofing, social engineering etc.) • Web defacements • Hacking of IT systems such as computers systems, Servers (Mail, Web, Database etc) and Routers • Application level attacks • Denial of service attacks (DoS) • Distributed Denial of Service (DDoS) • Attempts for exploitation of zero-day vulnerabilities • Detection of new and advanced malware infections
Level 2 **Elevated** **Scope:** **Multiple Organisations**	Perceptible change/variation in network/ system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organisations/departments simultaneously due to: • Large scale infection of viruses/worms/ Bots/malware/ Keyloggers/Spyware for malicious and espionage activities • Focused attempts of network scanning and penetration • DoS/DDoS attacks • Attacks on Domain Name Servers, Mail Servers, Databases, Routers etc • Attacks on Web servers resulting in defacement of websites on large scale • Attacks on Trusted infrastructure • Attack on the IT infrastructure of a Critical Information System • Infection of computer systems and/or Programmable Logic Controllers (PLCs) • Abnormal functioning of SCADA/Industrial Control Systems

Level 3 **Heightened** **Scope:** **State/** **Multiple States**	Significant breakdown of supplies or services essential to the life of the citizens *including but not limited to* financial, Government, transport, energy or communication due to focused cyber attacks on infrastructure of critical sector and Government across a state or multiple states.
Level 4 **Serious** **Scope:** **Entire Nation**	Significant/complete breakdown of supplies or services essential to the life of the citizens *including but not limited to* financial, Government, national defence, transport, energy or communication due to focused cyber attacks on infrastructure of critical sector and Government across the nation.

Appendix-N

Eligibility criteria for Head CERT-O:

Minimum 15 years of working in related field or Govt. Officer dealing with IT/Cyber crime matters/data management not below the rank of Dy Secretary.

Eligibility Criteria for Security Expert

Essential:

a) First Class Engineering Graduate in B-Tech/M-Tech/ MCA / M.Sc (IT)

b) CISA/CISSP/ CASM/ BS7799LI Certification.

Desirable:

- Hands on experience on managing Information Security System devices.
- Exposure to formulate and implement Information Security Policies and Procedures.

Experience:

Minimum 5 years of working experience in a Bank/ Financial/ Govt / Large IT Institution of which minimum 3 years of experience in Information Security domain out of which 2 years as Information Security Officer / Information Security Offices or at equivalent position.

Broad Skill Set Required:

1. Demonstrate an understanding of comprehensive security programs, including technologies and tools, architectures and network and application design and policies/business aspects of risk.
2. Able to assess, develop and implement information security programs including organizational design and key processes/procedures.
3. Demonstrate extensive knowledge of information security standards: ISO27001, ITIL, NIST, SANS.
4. Understanding of IT requirements of the industry.

Appendix-O

I. *Internal Stakeholders:*

National Informatics Centre

1. **NIC HQ, New Delhi**
   - HOG, Cyber Security Group, NIC, A-Block, C.G.O Complex, Lodhi Road, New Delhi,
     Email: security@nic.in
2. **NIC OSU, Odisha**
   - DDG & SIO (S.K. Panda),NIC, Odisha State Unit, Sachivalaya Marg, Unit IV, Bhubaneshwar, Odisha,
     Tel : 0674-2508438,E-Mail : sio-ori@nic.in
   - HO & Data Centre Incharge (C.R. Kanungo), NIC, Odisha State Unit, Sachivalaya Marg, Unit IV, Bhubaneshwar, Odisha,
     Tel : 0674-2508329, E-Mail : crkanungo@nic.in

II. *External Stakeholders :*

Type of stakeholders	*Name*	*Contact Details*
ISP	a) BSNL b) Railtel c) STPI d) NIC e) Reliance f) Airtel g) Ortel h) Sify	
Telecom operator	*a) BSNL* *b) Airtel* *c) Aircel* *d) Vodafone* *e) Reliance* *f) Tata Docomo*	
Law enforcement Agency		

Appendix-P

SOP for Website Defacement

Case Study: Defacement of the State Portal

The Standard Operating Procedure (SOP) comprises of the following steps:

I. **Preparation Stage :**

a) After reporting of the incident by user it is forwarded to the Head (State Portal)
b) It is then forwarded to the sectoral CERT(CERT-O)
c) CERT-O analyses the website at the basic –level
d) Setting up of tools for further analysis
e) Following the BCP (Business Continuity Plan) to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.
f) Pulling the website down if the incident is found to be severe for analysis & further resolution.

II. **Identification Stage :**

a) Ensuring incidents - Monitor web pages - Reports from users - Use a tool (Zone-h)
b) Detecting source - Static files - Components mashups - Links page - Log file
c) Check for malware
d) Checking the contents of the database
e) Measuring the impact

III. **Containment Stage :**

a) Back up all data on the web server
b) Inspect and inventory all components of a web server system
- Services
- Ports
- Vulnerability (write access to the file)
- Vulnerability in SQL codes
- Vulnerability of web programming code
- Folders are public
- The presence of malware
c) Checking connectivity with other system
d) Seeking and finding the source of the attack
e) Breaking the connection with the source of the attacker
f) If the problem is difficult to solve – Creation of new webpages
g) Document the tracing process for future incidents

IV. **Eradication :**

a) Erase
- All of the content that may be infected malware (Trojan, rootkit)
- Web content that has been defaced
- Suspicious application
b) Restoring all the database to the web from a backup Clean
c) Patching and updates
- CMS web builder
- A web server (Apache, IIS)
- Operating System server (Linux, Windows)
d) To examine the susceptibility to see the gap that still exists

V. Recovery Stage :

a) Replacing all of the components /builders on the web
b) Reactivate web page
c) Renew all user authentication
d) Mapping and closing all vulnerabilities that have been identified.
e) Public Explanation
f) Perform Penetration Testing

VI. Closure Stage :

a) Creating Activity report
b) Creation of new knowledge base
 - Engineering attacks
 - Weakness of the web server
c) Document Root Cause Analysis
 - Records evidence
 -Take note of the tools used
 -Making analysis and explanation
d) Making evaluation and recommendation

Further SOPs will be prepared for different types of crisis by CERT-O in due course of time to deal with them efficiently.

ORDER

Ordered that the Notification be published in an Extraordinary issue of the *Odisha Gazette* and copies of the Notification be forwarded to all Departments of Government.

By Order of the Governor

P. K. JENA
Principal Secretary to Government

Abbreviations

ADSL……………….Asymmetric Digital Subscriber Line

ACISO……………..Additional Chief Information Security Officer

CMP……………….....Crisis Management Plan

CCTNS…………….Crime and Criminal Tracking Network & Systems

CERT – In…………Computer Emergency Response Team – India

CERT – O……….. Computer Emergency Response Team – Odisha

CISO………………Chief Information Security Officer

DNS………………..Domain Name Service

ISO………………… Information Security Officer

ISP………………….Internet Service Provider

IT……………………Information Technology

LAN…………………Local Area Network

MoD………………..Ministry of Defence

NIC………………...National Informatics Centre

NIXI……………….National Internet Exchange of India

NCSP ……………..National Cyber Security Policy

NTRO……………...National Technical Research Organisation

NCMC…………..….National Level Crisis Management Committee

OCAC……………..Odisha Computer Application Centre

OSDC……………..Odisha State Data Centre

OPSC.................. Odisha Public Service Commission

OSWAN…………..Odisha State Wide Area Network

PSU………………..Public Sector Unit

SAMS……………...Student Academic Management System

SCMC……………...State Level Crisis Management Committee

SMTP………………Simple Mail Transfer Protocol

SeMT………………State e-Governance Mission Team

UID…………………Unique Identification

Wi-Fi……………… Wireless Fidelity

WiMAX…………….Worldwide Interoperability for Microwave Access

Printed and published by the Director, Printing, Stationery and Publication, Odisha, Cuttack-10
Ex. Gaz. 572-173+500